HWG | HARRIS, WILTSHIRE & GRANNIS LLP

November 17, 2021

REQUEST FOR CONFIDENTIAL TREATMENT

Via ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th St SW
Washington, DC 20554

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, ET Docket No. 21-232

Dear Ms. Dortch,

Pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, Hikvision USA, Inc. ("Hikvision") hereby requests the Commission withhold indefinitely from any future public inspection and accord confidential treatment to the company-specific, confidential, business sensitive information contained in the accompanying report that is being submitted in conjunction with this request.

The Confidential Information constitutes highly sensitive, commercial information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"). Exemption 4 of FOIA provides that the public disclosure requirement of the statute "does not apply to matters that are . . . (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. § 552(b)(4). Because this information is provided on a voluntary basis in support of Hikvision's *ex parte* and is "of a kind that would customarily not be released to the public," it is "confidential" under Exemption 4 of FOIA. *See Critical Mass Energy Project* v. *NRC*, 975 F.2d 871, 879 (D.C. Cir. 1992).

In support of this request and pursuant to Section 0.459(b) of the Commission's rules, Hikvision hereby states as follows:

1. Identification of the Specific Information for Which Confidential Treatment Is Sought (Section 0.459(b)(1))

Hikvision seeks confidential treatment of the information identified as confidential in its accompanying report, which has been redacted from the public versions of that document.

2. Description of the Circumstances Giving Rise to the Submission (Section 0.459(b)(2))

Hikvision is submitting the confidential information in its accompanying report as part of the Commission's rulemaking proceeding in the above-captioned matter.

3. Explanation of the Degree to Which the Information Is Commercial or Financial, or Contains a Trade Secret or Is Privileged (Section 0.459(b)(3))

The confidential information is exempt from disclosure because it contains commercially sensitive information. In particular, some of the confidential information includes a security analysis of Hikvision's products, disclosure of which may tend to increase the likelihood of a successful cyberattack on Hikvision equipment.

4. Explanation of the Degree to Which the Information Concerns a Service that Is Subject to Competition (Section 0.459(b)(4))

The confidential information is related to the provision of video surveillance and network video recorder services, which is a highly competitive industry.

5. Explanation of How Disclosure of the Information Could Result in Substantial Competitive Harm (Section 0.459(b)(5))

Disclosure of the confidential information could harm Hikvision if it were to enable a successful cyberattack.

6. Identification of Any Measures Taken to Prevent Unauthorized Disclosure (Section 0.459(b)(6))

Hikvision routinely treats the confidential information provided in the accompanying report as highly confidential and exercises significant care to ensure that such information is not disclosed to its competitors or the public.

7. Identification of Whether the Information Is Available to the Public and the Extent of Any Previous Disclosure of the Information to Third Parties (Section 0.459(b)(7))

Hikvision does not make this information public and has not previously disclosed it to third parties.

8. Justification of the Period During Which the Submitting Party Asserts That Material Should Not Be Available for Public Disclosure (Section 0.459(b)(8))

Hikvision requests that the confidential information be withheld from public disclosure on an indefinite basis because confidential treatment is required to secure the cybersecurity of Hikvision products and protect Hikvision's end users.

Sincerely,

John T. Nakahata
HARRIS, WILSHIRE & GRANNIS LLP
1919 M Street, N.W.
Eighth Floor
Washington, DC 20036
Tel: (202) 730-1300
Fax: (202) 730-1301

Counsel to Hikvision USA, Inc.

HIKVISION EQUIPMENT CYBERSECURITY ASSESSMENT REPORT

PUBLISHED NOVEMBER 12, 2021

FTI Cybersecurity

An Intelligence-Led, Expert-Driven, Strategic Approach to Global Cybersecurity Challenges

Prepared for Hangzhou Hikvision Digital Technology Co., Ltd.

Confidential

II. Executive Summary

FTI Consulting's cybersecurity assessment of the selected Hikvision equipment concluded the devices present no immediate concerns for the end-user in any use-case environment. FTI determined that the communications between the devices and to/from the Hikvision servers were consistent with normal operation. Furthermore, FTI's testing and analysis did not detect any Commonly Available Vulnerabilities and Exposures (CVEs) on either device or the ability for an unauthorized party to access the video transmissions. However, FTI's source code review of Hikvision's supporting software revealed two errors in code that caused communication to an outdated feature and to Hikvision servers outside of the intended geographical region. Finally, FTI identified specific recommendations that Hikvision could implement to further enhance the cybersecurity posture of their equipment, services, and to benefit the end-user.

Key Findings

FTI highlights the following key findings identified during the analysis of the two devices:

1) **Data Transmission**: FTI did not identify any unusual or unexpected data transmissions occurring with the identified equipment. FTI concluded that the NVR and Camera do not attempt to automatically establish a connection to Hikvision or other servers, even if they are configured to face out to the Internet. In addition, when there is no established Internet connection, the devices use the Multicast Domain Name Service (mDNS)[10] to detect specific hosts (i.e. other Hikvision devices) on their internal network to set up a dedicated connection to communicate as necessary. FTI did not identify any non-Hikvision device host requests within the mDNS traffic, indicating data transmissions were consistent as expected.

    a. **Hik-Connect:** On both the iOS and Android platforms, Hikvision implements an enhanced server authentication method through the use of SSL Pinning[11] at the time of log in [redacted]. This led to [redacted] however the password remains encrypted. FTI was only able to [redacted] SSL Pinning would [redacted]. None of this information was found in transmission [redacted]. Finally, based on the analysis of network traffic, FTI believes Hik-Connect uses its servers to facilitate an encrypted peer-to-peer[13] connection directly between the Hikvision devices and the user devices with Hik-Connect installed.

[10] Multicast DNS is used to resolve internal requested hostnames, such as other Hikvision devices. This is common practice for devices that are meant to communicate with other devices on the network. In this context, the NVR and Camera are searching for each other in order to alert and prompt the end user to add the camera to the list of the devices.

[11] SSL Pinning: This is an authentication enhancement where an App will bundle the known server certificate with itself to compare against the certificate received by the server to validate the connection if they match.

[12] Broadcasting Wi-Fi router name.

[13] A direct connection between two hosts or devices.

b. **iVMS-4200:** Upon loading iVMS-4200, FTI identified multiple connections to servers located in China. These connections occur at time the application is started by the user. (See Key Findings #8-Source Code for further information)

2) **Hikvision Server Hosting:** FTI concluded that Hikvision uses numerous Internet Service Providers (ISPs) within the United States for all Hik-Connect traffic. These ISPs included Amazon AWS (AMAZON-AES, AMAZON-02, Amazon Technologies Inc., Amazon.com, Inc.), Shenzhen Tencent Computer Systems Company Limited, Chinanet, CT-hangZhou-IDC, and Hangzhou Alibaba Advertising Co., Ltd. iVMS-4200 was the only application FTI identified using servers[14] hosted in China. The ISPs located in China are Chinanet, CT-hangZhou-IDC, and Hangzhou Alibaba Advertising Co., Ltd. (See Key Findings #8-Source Code for further information).

3) **Device Setup and Use Case:** Hikvision does not require devices to be configured in a specific way. Rather, users have the flexibility to configure their Hikvision devices in a number of ways to meet specific organizational requirements or utilize existing network infrastructure. FTI evaluated different setup configurations for each Hikvision device, including configurations that did not require Internet connectivity and were completely segregated from the network, known as an air-gapped environment[15]. When connected to the Internet, it is the responsibility of the end-user to ensure the devices are configured behind a security appliance such as a firewall. FTI recommends, as is standard with most Internet of Things (IoT) devices[16] in a corporate environment, to (1) establish a virtual local area network (VLAN) segregation between a Hikvision Camera, NVR, and other devices within the network, (2) configure a firewall to prevent unauthorized inbound and outbound network traffic, and (3) enable as many built-in security features as possible[17].

   a. FTI did not find information regarding the various device setup configurations available to the user in the documentation provided with the device upon purchase. FTI recommends that Hikvision present the user with more information about the configurable features of the device in the accompanying user manuals and documentation. (See Key Findings #10-Cybersecurity Best Practices for further information).

   b. When configuring a device with Hik-Connect, a user must assign a decryption password on the Hikvision device. The password is then used to unencrypt the video feeds on the Hik-Connect device being used to view the feeds. FTI attempted to intercept the password during both the setup and decryption, however, the data remained secure.

4) **Hardware Schematic:** FTI identified no inconsistencies in the hardware schematic design, design rules, schematic conventions, and documentation. FTI assesses that the Hikvision's schematic diagrams are of a high-quality design and engineering work product.

[14] Hangzhou Alibaba Advertising Co., Ltd.

[15] An air gapped environment is an environment either logically or physically segregated from the Internet.

[16] IoT devices will usually run outdated open-source packages and very light-weight versions of Linux leaving them prone to attacks if not secured properly.

[17] See Appendix A.

5) **Device Updates:** During testing, FTI noted that the NVR has an "auto-update" feature. At no point during network traffic capture did FTI record any traffic which indicated update checks were occurring. Auto-updates are a common feature in Internet-connected devices and are beneficial for helping end-users keep their Hikvision equipment operating with the most current firmware. FTI upgraded firmware versions one at a time to validate if the "auto-update" feature not functioning was related to the default firmware the device was shipped with. FTI confirmed that the "auto-update" feature did not activate through any iteration of firmware upgrade. Through inquiry with Hikvision, FTI learned that the "auto-update" feature is enabled for critical updates only and that updates are not automatically sent to end-user devices. Rather, regardless of how the device is configured, the end-user/owner must monitor for software updates and flash (update) the firmware manually. FTI recommends Hikvision enable the "auto-update" feature to ensure that all Internet-connected Hikvision devices automatically receive update notifications.

6) **Open-Source Software Packages and Vulnerability Assessment:** FTI identified the use of numerous open-source packages with outdated versions on both devices. Third-party reporting on Hikvision's use of these open-source software packages references multiple publicly known vulnerabilities associated with the individual software packages[18]. The third-party reporting references a report[19] by the Lithuanian National Cyber Security Centre (NCSC) alleging that Hikvision utilizes software solutions with 95 known Common Available Vulnerabilities and Exposures (CVEs). However, open-source software is routinely used and often altered by manufacturers to utilize only certain functionalities, eliminate unneeded features, and mitigate known vulnerabilities. Hikvision indicated that the open-source software packages it integrates into its camera software and firmware are encompassed in a "secure shell" and incorporate compensating controls to prevent any tampering and mitigate the publicly known vulnerabilities. FTI's vulnerability assessment scans concluded that none of the vulnerabilities present in the outdated packages were present on the devices further validating Hikvision's assertion and contradicting the allegations made against Hikvision in the third-party and NCSC reporting. Although not considered CVEs, FTI scans did find the use of outdated JavaScript libraries, IP-forwarding enabled, and the absence of Content Security Policy (CSP) implementation. However, the overall results of FTI's vulnerability assessment still indicate a low risk to the confidentiality, integrity, and availability of Hikvision hardware and data. This determination is based on the following factors:

   a. The outdated JavaScript packages do not introduce any known publicly available vulnerabilities,
   b. IP-forwarding presents a very small attack surface and is mitigated by proper configuration by the end-user, and

[18] https://ipvm.com/reports/hikvision-lithuania-vuln?code=allow
[19] https://d1tzzns6d79su2.cloudfront.net/uploads/embedded_file/e6609d3b6aa299918f6d1ae5e3c802d57bd25cdcf7db2565baa27095e32c8af0/a94cee92-c8e6-45d0-a1ec-ef5f7dbc2761.pdf

c. While the CSP implementation does provide a layer of defense against Cross Site Scripting and data injection attacks, these threats are mitigated with proper configuration by the end-user.

7) **Firmware Signature Integrity:** During the source code review, FTI found that Hikvision conducts an integrity check at the time of updating the device. Integrity checks are utilized to detect if unauthorized changes have been made to the updated firmware. FTI found this to be true regardless of how the user chooses to update the device.

8) **Source Code:** During FTI's examination of cybersecurity centric features available on Hikvision's devices at Hikvision's headquarters' offices in China, FTI determined that the logic surrounding each function was correct, did not have any mistakes, and was functioning as intended. FTI's examination of communication protocols and destinations identified the source of the Chinese-based connections on iVMS-4200 which were connections associated with identifying software updates. During the source code analysis, FTI was able to determine that these connections were caused by either incomplete or outdated functions that had not been fully removed. Further conversations with Hikvision developers helped FTI understand that this was the result of an outdated function used to connect with an old Alibaba hosting service that has now come to end-of-life. FTI also worked with Hikvision developers to identify an incomplete function that is meant to overwrite a default configuration file with a regional-based configuration file. Hikvision presented updated source code for both functions to FTI showing the removal of the outdated function and a fix for the incomplete function. Per Hikvision developers, both function corrections will be included in a future update of iVMS-4200.

9) **Hik-Connect Authentication:** During the source code review, FTI identified that the MD5[20] cryptographic hashing algorithm[21] is being used to authenticate accounts. MD5 is known to have vulnerabilities and is not recommended to be used for authentication mechanisms. FTI recommends implementing a different hashing algorithm, such as SHA-256[22] with salt[23] as a replacement to the current MD5 hashing algorithm.

10) **Cybersecurity Best Practices:** Support, resources, and advice on how to properly harden and configure Hikvision hardware is available on the Hikvision Cybersecurity Center webpage. Hikvision should consider including this guidance as well as cybersecurity best practices and possible configurations for the devices in the package contents for their devices.

[20] MD5 is a type of cryptographic hashing algorithm. MD5 is considered end of life as collisions can now be calculated in seconds.
[21] A cryptographic hashing algorithm is a mathematical algorithm used to determine the arbitrary size to a fixed value of bytes. It is a one-way function which is practically near impossible to reverse. Cryptographic functions are commonly used to transmit and store passwords.
[22] SHA-256 is a type of cryptographic hashing algorithm.
[23] Salt is a cryptographic enhancement to a hashing algorithm used to safeguard passwords in storage.